УДК 65.011.3

АНАЛІЗ FREAK АТАКИ ЧЕРЕЗ ВРАЗЛИВІСТЬ «CVE-2015-0204»

Колгін Володимир Андрійович[1], Масальська Олена Олександрівна
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: vovik425@gmail.com[1]

Ця стаття призначена для ознайомлення з новою атакою на основі MITM-атаки, аналіз її реалізації, алгоритм та умови атаки.

Ключові слова – MITM-атака, HTTPS-протокол, OpenSSL

ВСТУП

Дослідники з INRIA (національний дослідницький інститут у Франції, що працює в галузі комп'ютерних наук, теорії управління та прикладної математики) і Microsoft повідомили про виявлення уразливості під номером CVE-2015-0204, яка, імовірно, існувала протягом більш ніж 15 років і яка робить технічно можливим перехоплення HTTPS-трафіку, який йде між певними сайтами і пристроями під керуванням Apple iOS і MacOS, а також Google Android.

FREAK - це абревіатура від Factoring attack on RSA-EXPORT Keys. Атака спрацьовує, коли вразливі пристрої підключаються до сайтів, на яких стоїть морально застаріле програмне забезпечення для шифрування, яке, як вважалося, вже давно ніким не використовується. Зловмисник, який має можливість перехоплювати трафік між вразливим пристроєм і вразливим сервісом, може впровадити в нього свої спеціальним чином створені пакети, які змусять обидві сторони використовувати "для спілкування" слабкий 512-розрядний ключ для шифрування. Змусити браузер і сайт перейти на більш низький рівень шифрування - ключовий момент FREAK-атаки.

Після цього зловмисник може використовувати орендовані на, наприклад, Amazon, обчислювальні потужності для того, щоб легко дешифрувати слабкий за нинішніми мірками ключ, схований у перехопленій трафіку. За оцінками фахівців, вартість потужностей, потрібних для такої операції складає близько 100 доларів, що робить FREAK привабливим для хакерів-аматорів, а професіоналам дозволяє поставити злом "на потік". Розкривши ключ, зловмисник може "підняти" в локальній мережі або, наприклад, в Wi-Fi-мережі кафе, копію даного його сайту і збирати різну інформацію - логіни і паролі від соціальних мереж, ключі від інтернет-банків і так далі.

Попутно вимальовується кілька додаткових проблем, які роблять FREAK дуже ефективною атакою. По-перше, генерувати нові RSA-ключі - дороге задоволення, тому багато веб-сервери, стартуючи, генерують один єдиний ключ, який потім використовують для захисту всіх з'єднань. Якщо зловмисник його перехоплює - він може ним користуватися "всю дорогу".

По-друге, HTTPS-протокол не вимагає від учасників з'єднання відмови від використання 512-бітних ключів, в результаті чого останній є цілком "валідним" для спілкування між сервером і клієнтом. Навіть, незважаючи на те, що сучасні обчислювальні потужності дозволяють його зламати хакерам-любителям за розумний час.

ПРИЧИЕВ ВИНИКНЕННЯ УЯЗЛИВОСТІ

Адміністрація президента Білла Клінтона, яка в 1990-х роках заборонила експортувати з США криптографічні алгоритми та пристрої певної "потужності". В результаті слабкий 512-розрядний ключ став стандартом де-факто - і залишається ним навіть сьогодні, коли заборони на експорт криптографічних технологій вже давно немає. Стандартом він став просто тому, що спочатку всі хотіли, щоб з їх сайтами і технологіями взаємодіяло якомога більше людей, включаючи і іноземців, позбавлених криптографічної мощі США.

УМОВИ АТАКИ

З'ясувалося, що в реалізації OpenSSL (Браузер в Android) і Apple TLS / SSL (Safari) існує баг, який дозволяє «людині посередині» змусити клієнта використовувати EXPORT-шифрування, навіть якщо клієнт не заявляв про його підтримку. Для цього повинні виконуватися відразу декілька умов:

Клієнт використовує вразливу версію OpenSSL або Apple TLS / SSL

Підтримка EXPORT-шифрування включена на сервері

Наявність закритого ключа RSA 512 біт у зловмисника

Для того, щоб експлоїт спрацював, вразливе пристрій повинен підключатися до уразливого сайту. І "спілкування" між ними повинно проходити в мережі, до якої у зловмисника є доступ. Якщо Ваш пристрій не вразливий, або сайти не уразливі, або не можна фізично перехопити трафік - у зловмисника нічого не вийде. Однак, наявність одночасно і великої кількості пристроїв, і величезної кількості сайтів (приблизно на 36.7% із загальної маси сайтів і на 9.7% з мільйона найбільших сайтів) робить FREAK однією з найбільш небезпечних атак з усіх, що були виявлені за останній час. Що до перехоплення трафіку - багато людей користуються безкоштовним Wi-Fi і поняття не мають, як їм захистити свої домашні мережі.

МОЖЛИВІ ЗБИТКИ

Атака дозволяє зловмисникам відносно легко отримувати логіни і паролі від сайтів, інформацію з Інтернет-банків, зміст поштових повідомлень і так далі. Вони можуть отримати все, що ви відправляєте на / через сайти, які захищені HTTPS-з'єднанням.

ЯК ЗАХИСТИТИСЯ ВІД АТАКИ FREAK

На стороні клієнта вразливість зачіпає OpenSSL (виправлено в 0.9.8zd, 1.0.0p і 1.0.1k), браузер Safari і різноманітні вбудовані та мобільні системи, включаючи Google Android і Apple iOS. Що стосується серверів, то сканування мережі показало, що набір RSA_EXPORT підтримується приблизно на 36.7% із загальної маси сайтів і на 9.7% з мільйона найбільших сайтів. Для захисту сервера на базі Apache до параметрів директиви SSLCipherSuite слід додати "! EXPORT".

ВИСНОВКИ

У WEB – світі багато вразливостей, які можуть бути сховані на багато років, але одного дня вони заявляють про себе усьому світі та загрожують безпеці персональних даних мільйонів користувачів інтернет. Будьте обачливими та серйозно відноситься до вашой віртуальної безпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стаття: портал DELFI (Електрон. ресурс) / Спосіб доступу: URL: http://rus.delfi.lv/news/daily/story/istoriya-dnya-vse-pro-freak-novuyu-katastroficheskuyu-bresh-v-ustrojstvah-apple-i-android.d?id=45648354.
2. Стаття: блог лабораторії Касперского (Електрон. ресурс) / Спосіб доступу: URL: http://blog.kaspersky.ru/chto-takoe-chelovek-poseredine/740/.
3. Доклад: форум (Електрон. ресурс) / Спосіб доступу: URL: http://provisionsecurity.ru/threads/674/